Volume 4, No. 2, Jan-Feb 2013

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

"Near Field Communication"- An Enhanced Approach Towards Contactless Services

Piyush Suthar*
Department of Information Technology
Parul Institute Of Engg. & Technology
Waghodia, India
Piyush.s.suthar@gmail.com

Neha Pandya
Department of Information Technology
Parul Institute Of Engg. & Technology
Waghodia, India
neh.pandya@gmail.com

Abstract: This paper is based on research of current aspects of security in Near Field Communication. The Near Field Communication (NFC) mobile service, which leverages the current contactless infrastructures, has just started to emerge. In some countries, services benefiting from the convergence of contactless card technology and mobile phones have already been introduced commercially, and these services got somewhat acceptance also. NFC enables quick and secure functionality in numerous areas including mobile contactless payment, ticketing and data transfer. Smart phones are becoming omnipresent as their adoption increases due to the convergence of value-added services in them including Near Field Communication (NFC). Though NFC based services are not yet widely accepted, this paper provides the insights for the technology, challenges are reported and finally future directions are suggested for technology to breathe.

Keywords: Near field Communication (NFC); contactless; Security aspects; RFID; Universal Integrated Circuit Card (UICC)

I. INTRODUCTION

Contactless is a term defined by the Smart Card industry. It applies to short distance communications between two devices that are not physically connected. This permits development of contactless services. Many different variations of "Contactless technology" exist today one of them is Near Field Communication (NFC) technology. NFC is designed to operate over very short distances, typically less than 4 cm and provides a fast, simple and secure means for the user to experience a range of new contactless services with their mobile phone. The technology incorporates the ISO 14443 Type A and Type B standard for RFID technology that uses interface of a smartcard and a reader into a single device that is based on RFID technology [1]. It allows us to transfer data within few centimeters. One of the advantages of NFC over other wireless technologies is simplicity, transactions are initialized automatically after touching a reader, another NFC device or an NFC compliant transponder. Due to its simplicity, it has become a new and exciting area for practitioners [2].

A. Specifications:

NFC is operating at the radio frequency ISM band of 13.56 MHz. The communication range of NFC devices is approximately 10 cm. The NFC interface and protocol standard derives three different bit rates that are: 106, 212 and 424 Kbit/s [2].

B. Communication modes:

NFC operates on two communication modes: *Passive Communication Mode*: Only the initiator generates the RF field. The target answers in a load modulation scheme. It is an extended mode for p2p and RFID communication; here target device acquires the operating power from the Initiator-provided electromagnetic field. *Active Communication Mode*: Both the initiator and the target generate RF. It is the Standard mode for peer to peer (p2p) communication. In this mode, both devices have their own operating power [3].

C. Standards:

NFC was approved as an ISO/IEC standard on December 8, 2003 and later as an ECMA standard. NFC is an open platform technology standardized in ECMA-340 and ISO/IEC 18092. NFC incorporates a variety of existing standards including ISO/IEC 14443 both Type A and Type B. NFC enabled phones work basically at least, with existing readers. Especially in "card emulation mode" a NFC device should transmit, at a minimum, a unique ID number to an existing reader [3].

a. NFC Forum: The Near Field Communication Forum was formed to advance the use of Near Field Communication technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology. It formed in 2004. The goals of the NFC Forum lies in Developing & encouraging standards-based NFC specifications that define a modular architecture and interoperability parameters for NFC devices and protocols, also it works to ensure that products claiming NFC capabilities comply with NFC Forum specifications, finally it provides framework for NFC application development [4].

***b. GSMA*:** The GSMA represents the interests of mobile operators worldwide. Spanning more than 220 countries, the GSMA unites nearly 800 of the world's mobile operators with more than 230 companies in the broader mobile ecosystem [5]. It launched the following initiatives relating to NFC. *The Mobile NFC initiative*: It formulates point of view of mobile operators on the NFC ecosystem. *The Pay buy mobile initiative*: It seeks to define a common global approach to using Near Field Communications technology to link mobile devices with payment and contactless systems [11].

c. ***UICC:*** Mobile NFC is defined as the combination of contactless services with mobile telephony, based on NFC technology. The mobile phone with a hardware-based secure identity token (*UICC- Universal Integrated Circuit Card*) can provide the ideal environment for NFC applications. The UICC can replace the physical card thus optimizing costs for the Service Provider, and offering users a more convenient service. Figure 1 illustrates the working of NFC enabled UICC.

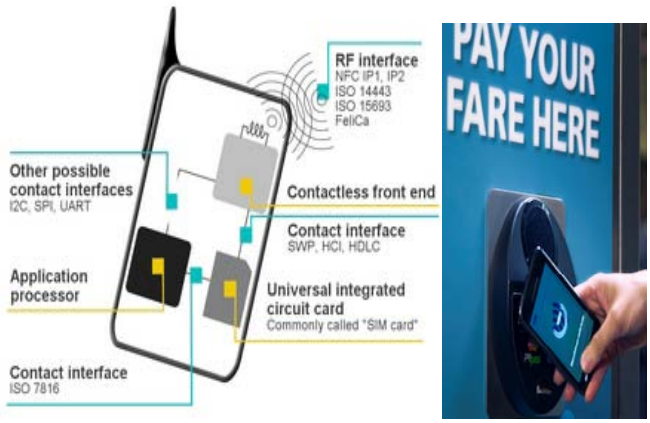

Figure.1 Basic working of UICC Mobile Phones in NFC [7]

Strategy Analytics forecasts that mobile phone based contactless payments will facilitate over $45 billion of worldwide consumer spending by 2012.

D. NFC Modes of Operation:

The NFC Forum [4] has created specifications for NFC devices, on which NFC devices can operate in three different modes based on the ISO/IEC 18092, NFC IP-1 and ISO/IEC 14443 contactless smart card standards. These are: card *emulator; reader/writer and peer-to-peer*. In card-emulation mode the data is transferred from mobile-device to NFC-Reader; in reader/writer mode data is transferred is from NFC tag to mobile device or mobile device to NFC tag; and in peer-to-peer mode data is transferred between two NFC compatible devices [12].

E. Applications:

It is not possible to enlist all NFC applications exactly as NFC provides just an interface. From the perspective of its practical use and real life applications, the operation modes of these NFC enabled devices can be generally classified into following categories.

a. ***Card emulation mode:*** The card emulation mode eliminates the need of carrying any physical object like credit cards, keys and coupons. Here one NFC mobile may even store multiple contactless smart card applications concurrently. Consider two applications, payment and electronic key as examples. In payment case; user is able to pay with her mobile phone while others should pay using cash or credit card in older methods. So NFC-payment is able to eliminate carrying cash or credit and debit cards. In e-key case; user can enter her hotel's room by opening the door with her e-key which is installed to her mobile device by SMS before arrival. Also she can check-out using NFC technology. The Symbian and Java implementation for NFC does not currently support this mode of operation. NFC electronic key application is able to eliminate a physical object such as physical key, but also is able to provide access control, since it provides an authentication mechanism. Another example that provides access control is attendance control, which authenticates students while attending to class. We can say that identified benefits of this mode are elimination of carrying a physical object and obtainment of access control [12].

b. ***Reader/writer mode:*** This mode provides communication of an NFC mobile with an NFC tag. The purpose of the communication is either reading or writing data from or to a tag by the mobile phone. We can further categorize the mode into two different modes: reader mode and writer mode. In reader mode, the mobile reads data from an NFC tag; whereas in writer mode, the mobile phone writes data to an NFC tag. Many applications are developed using this mode. Smart poster applications are one of the most important applications of this mode and in a university smart poster application is presented. In this application users are able to read data from NFC-enabled posters using their NFC-enabled mobile devices. Upon receiving a data to mobile device (e.g. a department staff information), she can walk away from the poster but she can still read data from mobile device. She doesn't need to write down the data to a paper neither she doesn't have to remember it which can still be read at the screen. As described above, user gained mobility from this process as she can get the required data to mobile device and leave the location. In, patients uploaded their medical information using NFC technology from their homes [12]. Increasing power of the mobile and its improving internet access has helped make this mode more attractive. In the other smart poster application [13], smart posters were used to give information to students, staff and faculty.

c. ***Peer-to-peer mode:*** Fewer applications are developed using peer to peer mode rather than other mode's applications. When one device is transmitting, the other has to listen and can start transmitting data after the first one finishes. Peer-to-peer mode is less used when compared to other modes, though it is studied for device pairing, networking and file transfer operations. Users manually select the option of adding a friend and then touch the other person's device with their own. In, Bluetooth pairing is achieved between the mobile phone and the car's hands-free equipment. In users exchanged their business cards by touching their NFC-enabled mobile phones to each other.

II. SECURITY ASPECTS AND CHALLENGES OF NFC

In NFC, due to its short range user privacy and man-in-the-middle attacks are two major concerns. By using special communication protocols, these problems can be overcome by NFC up to some extent.

A. Eavesdropping:

The RF signal for the wireless data transfer can be picked up by attackers with antennas. The distance from which an attacker is able to eavesdrop the RF signal, depends on numerous parameters, but is typically a small number of meters. Also, eavesdropping is extremely affected by the communication mode. A passive device, which does not generate its own RF field, is much harder to eavesdrop on than an active device. When a device is sending data in active mode, eavesdropping can be done up to a distance of about 10 m, whereas when the sending device is in passive mode, this distance is significantly reduced to about 1 m. The only real solution to eavesdropping is to establish a secure channel. Applications have to use higher-layer cryptographic protocols (e.g., SSL) to establish a secure channel [12].

B. Man-in-the-Middle-Attack:

In Man-in-the-Middle Attack, two parties which want to talk to each other are tricked via a three party conversation by an attacker. NFC link is not susceptible to a Man-in-the-Middle-Attack also it is not possible practically.

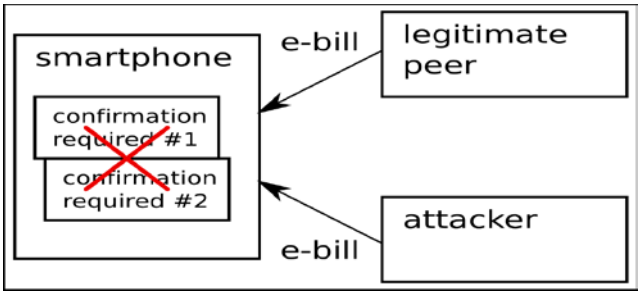

Figure. 2 Phenomenon of simultaneous payment [8]

As shown in fig. 2. When confirming a payment, there should not be two or more simultaneous payment requests from different payees, Figure 1; or, when payment is confirmed but the service is still unavailable, assume fraudulent use—the payment went to the wrong destination so the user should investigate.

C. Denial of Service:

Just touching an NFC device –even with an empty tag – causes a reaction of the device. Even if it is only an error message, this is a simply way to occupy the device. Also an attack could be implemented by using a sticky paper tag containing a malformed NDEF message and placing it on top of an NFC-tag belonging to the service that is to be discredited [12]. Thus there should be some kind of mechanism controlled by the user to turn on and of the NFC reader/writer functionality [6].

D. Phishing:

Phishing attacks could easily be performed by modifying or replacing tags. This is a simple and inexpensive way to mislead the user. Using signatures on tags and transporters would be suitable way to overcome this issue [6].

E. Relay attack:

In a relay attack the authentication protocol is bridged, such that authentication no longer requires physical proximity. Users transacting unique low-cost objects (such as people presenting movie tickets at the entrance) are particularly vulnerable to relay attacks. On the one hand, the low value of the transaction makes an interaction-free approach more acceptable. On the other hand, if the object owner is willing to publicly share the object, then she becomes vulnerable to malicious relaying of the ticket and involuntarily granting entry to an attacker. While relay attacks can be prevented by distance bounding, the technology is still in its infancy [8].

F. Data modification:

In data modification the attacker wants the receiving device to actually receive some valid, but manipulated data. This is very different from just data corruption [9]. There is no way to prevent such an attack, but if the NFC devices check the RF field while they are sending, it is possible to detect it.

The solution is to let NFC devices check the RF field while sending. This means the sending device could continuously check for such an attack and could stop the data transmission when an attack is detected [9].

III. SECURITY SOLUTIONS OVER THE CHALLENGES FOR NFC

To protect two NFC devices against eavesdropping and data modification attacks a secure channel establishment is worth considering approach as the Man-in-the-Middle attack cannot influence the NFC link. So use of techniques that has not any kind of provision of authentication is used to provide a standard secure channel.

The GSMA NFC Initiative facilitates financial transactions that require security, using a trusted service manager (TSM) between the service provider and mobile network operator layers [11]. The customer and the service providers approaches third party organizations that maintain the security data and other certain requirements like physical storage and protection.

IV. CONCLUSIONS

As all the new technologies, in NFC also security concerns still remains a big question. Nevertheless, the benefits of NFC mobile services are immeasurable. NFC-enabled devices can change the way we make transactions, exchange information, and send and receive data.

In 2011, the big names in mobile technology planned to integrate NFC with their new devices. Both Android and Blackberry already have or will have NFC-supported models; the media predicts that Apple will follow suit in its next generation of iPhones. The next few years will see more NFC support in mobile devices. Now this year in 2012 Sony introduces the "Smart Tags", which uses NFC technology to change modes and profiles on a Sony smartphone at close range, included in the package of (and "perfectly paired" with) the Sony Xperia P Smartphone released the same year [10], It'll be a matter of time before commerce, transportation, and other institutions develop the infrastructure to jump into the game. Considerations for successful NFC are Good NFC infrastructure, Low costs for contactless payments, developing free application on NFC, Single API for android market [2].

With different NFC applications, service is not yet well elaborated as NFC is failed against eavesdropping or data modifications. To achieve this a secure channel establishment is suggested. For further research, to further evaluate its potential, markets should be analyzed in terms of interest in NFC, market structure, and infrastructure readiness, its all won't work until the critical mass understands & accepts the technology.

V. REFERENCES

[1] Ortiz, C. Enrique "An Introduction to Near-Field Communication and the Contactless Communication API", 2008-10-24.

[2] Büsra ÖZDENIZCI1, Mehmet AYDIN2, Vedat COSKUN2 and Kerem OK2, "NFC Research Framework: A Literature Review And Future Research Directions", 14th IBIMA Conference, June 2010.

[3] Ecma International, "Near Field Communication - White Paper", url: http://www.ecma international.org/, Ecma/TC32-TG19, December 2005.

[4] NFC Forum: http://www.nfc-forum.org/news/pressreleases.

[5] The GSM Association (GSMA) : http://www.gsma.com.

[6] Gerald et. al., "NFC Devices: Security and Privacy", IEEE Reliability and Security,2008 [The Third International Conference on Availability]

[7] Raisonance- A Keolabs Company : http://www.sc-raisonance.com/nfctest.html, Mobile Ecosystem : http://www.mobile-ecosystem.org.

[8] Ben Dodson, Hristo Bojinov and Monica S. Lam, " Touch and Run with Near Field Communication (NFC)", Computer Science Department, Stanford University, October 2010.

[9] Ernst Haselsteiner and Klemens Breitfub ," Security in Near Field Communication (NFC) ", Philips Semiconductors, Printed handout of Workshop on RFID Security RFIDSec 06,Austira July 2006.

[10] Engadget:Sony Ericsson NFC Patent, http://mobile.engadget.com/2007/11/20/sonyericssons-patent-application-for-drag-and-dropnfc- style, 2007.

[11] GSMA, "Mobile NFC technical guidelines v2.0", Nov. 2007, white paper.

[12] Mohammed Riyazuddin., "NFC: A review of the technology, applications and security.", Information Technology Center, King Fahd University of Petroleum & Minerals, Saudi Arabia.

[13] I. L. Ruiz, M. A. Gomez-Nieto, "University Smart Poster: Study of NFC Technology Applications for University Ambient", Proc. 3rd Symposium of Ubiquitous Computing and Ambient Intelligence, Salamanca, SPAIN, Springer, 2008, pp. 112-116.